SSA-370042: Cross-Site-Scripting (XSS) in SICAM A8000 RTUs

Publication Date: 2020-08-11
Last Update: 2020-08-11
Current Version: V1.1
CVSS v3.1 Base Score: 8.3

SUMMARY

The latest update for SICAM A8000 RTUs fixes a vulnerability that could allow attackers with network access to the device's web server to perform a stored Cross-Site-Scripting attack.

Siemens has released an update for SICAM A8000 RTUs and recommends to update as soon as possible.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SICAM WEB firmware for SICAM A8000 RTUs: All versions < V05.30	Update to V05.30. Applying the update causes the device / module to go through a single restart cycle. https://support.industry.siemens.com/cs/ww/en/view/109780765

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Restrict access to port 443/tcp.

GENERAL SECURITY RECOMMENDATIONS

Operators of critical power systems (e.g. TSOs or DSOs) worldwide are usually required by regulations to build resilience into the power grids by applying multi-level redundant secondary protection schemes. It is therefore recommended that the operators check whether appropriate resilient protection measures are in place. The risk of cyber incidents impacting the grid's reliability can thus be minimized by virtue of the grid design.

Siemens strongly recommends applying the provided security updates using the corresponding tooling and documented procedures made available with the product. If supported by the product, an automated means to apply the security updates across multiple product instances may be used. Siemens strongly recommends prior validation of any security update before being applied, and supervision by trained staff of the update process in the target environment.

As a general security measure Siemens strongly recommends to protect network access with appropriate mechanisms (e.g. firewalls, segmentation, VPN). It is advised to configure the environment according to our operational guidelines in order to run the devices in a protected IT environment.

Recommended security guidelines to Digital Grid Products can be found at:

https://www.siemens.com/gridsecurity

PRODUCT DESCRIPTION

The SICAM A8000 RTUs (Remote Terminal Units) series is a modular device range for telecontrol and automation applications in all areas of energy supply.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2020-15781

The login screen does not sufficiently sanitize input, which enables an attacker to generate specially crafted log messages. If an unsuspecting victim views the log messages via the web browser, these log messages might be interpreted and executed as code by the web application. This Cross-Site-Scripting (XSS) vulnerability might compromize the confidentiality, integrity and availability of the web application.

CVSS v3.1 Base Score	8.3
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Emma Good from KTH Royal Institute of Technology for coordinated disclosure

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2020-08-11):	Publication Date
V1.1 (2020-08-11):	Update remediation to denote the necessity of a restart. Update mitigation to only allow restricted access to the system.

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/

terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.